OSET INSTITUTE

STATEMENT

Increasing Concerns About Amplified Threats to Voting Systems

July 14, 2022 Palo Alto, CA. Over the past three weeks the OSET Institute has been encouraged to offer its position on questions about the public, but unauthorized availability of certain intellectual property (IP) assets related to certified, installed and operational voting systems and the potential risk or threat to election security involving those voting system technologies. It has been suggested that such a statement could be helpful to courts, legal counsels, media, and other interested members of the public. Ten percent of our public benefit services is election cyber-security advisory, which we have provided to state and federal agencies including elements of the national security apparatus for over a decade. The Institute's nonprofit mission also includes public education about election administration technology. Our senior most technologists have decades of experience in the analysis, design, and engineering of cyber, digital, and information security systems and services. And our team is fortified with several veteran election administrators. Backed by those capabilities and experience, we provide the following statement on the topic of risks posed by unauthorized public disclosure of election technology IP assets.

The Situation

Recent news about Dominion's voting system products has created concern that these products are at increased risk for compromise. Specifically,

1. CISA has issued a security advisory;
2. There was a recent wholesale disclosure of Dominion voting technology, related IP, and data in Coffee County, GA by improper access; and
3. Proceedings of a Georgia lawsuit could potentially result (at some point) in wider availability of information about Dominion products.[1]

In the case of Coffee County, this included at least, but may not have been limited to, unauthorized acquisition and potential disclosure of disk images that contain all the data and software of an Election Management System (EMS). This is essentially the same type of information that was improperly obtained from Mesa County CO's elections office, and used as the basis for a quasi-technical report falsely claiming proof of a stolen election. In the Coffee County case, it remains unknown whether the acquisition and disclosure[2] of Dominion technology was less than, equal, or greater in breadth and depth, thereby exacerbating an already serious situation.

---

[1] To be clear, any disclosures here would be due to the Court releasing currently sealed documentation. There certainly is no intent to implicate any unauthorized disclosures or violations of protective orders by either party. Plaintiffs did perform a civic duty in tracking down and publicizing a breach by certain external non-governmental operatives abetted by insiders in Coffee County that occurred in 2020.

[2] It is also important to distinguish disclosure from publication; the first is bad enough, whereas the latter could be catastrophic. We are unaware of any publication in the Coffee County incident at this time, and it is unconfirmed how many have had access so far (i.e., recipients of a disclosure).

The Institute is seriously concerned about these unauthorized disclosures[3] of election technology IP and the concerns outlined in our opening raise two questions:

1. Will the Coffee County (or any jurisdiction) release make it significantly easier for adversaries to attack future elections, or attack voting systems used in them?
2. If so, should these releases be stopped and future releases prevented (*if possible*)?

The short answer is that these releases are *dangerous*, regardless of any difference of opinion among technologists about whether such disclosure would be significantly easier, slightly easier, or simply catastrophic. And they *must* be prevented at all costs. Yet, their potential availability on the public Internet makes prevention a nearly impossible task— the proverbial cat is out of the bag.

Given the very challenging threat environment described next, even the slightest increase in ease of attack is an increase that *must* be avoided.

The Threat Environment

The current threat environment is daunting. Consider:

- The basic design of current voting system products (Dominion included) makes them fundamentally vulnerable to cyber-attack to change code, inject code, and/or tamper with data.
    - Voting system components are not fundamentally different from a typical personal computer (PC): subject to the installation of malware, to accidental or malicious modification of original software, modification of critical data by malicious or tampered software.
- Every independent review of every voting system in the last 15-years has shown that these products not only have these fundamental security weaknesses, but also are rife with poor quality software and many vulnerabilities, including those that are described in the dry specifics of CISA's recent security advisory.
    - These findings apply not just to the voting machines that voters see, but also the election management system (EMS) that is the "back-office brains" of the entire voting system and its many parts.
- There are known flaws, vulnerabilities, exploits, and attackers.
    - Many known specific flaws, and many known attack vectors, including malware injection that can spread from EMS to voting machines or vice versa.[4]

---

[3] https://www.washingtonpost.com/investigations/2022/06/12/coffee-county-georgia-dominion-breach/

[4] The Election Management System (EMS) "sees" every record tagged with information that is unique to the jurisdiction. In the case of Dominion's Democracy Suite EMS, it also handles ballot definitions, so it must both read and write those records. In addition to ballot definitions and voting records, the EMS also leaks considerable information about the development environment used to create the EMS software. If, for example, the developers' network management suite used a version of SolarWinds with a certain release date (software subject to a massive attack recently), then an adversary would know the system might contain an exploitable back door. The same holds for the logging software. For our technical audience, one could, for instance, check to verify that unprintable "escape sequences" can be passed along to the server, which would thereby allow malicious software code to be injected when the EMS was operating to simply read and write records.

  - High quality cyber attackers who are more than capable of using these attack vectors.

- Typical counter-measures, including those recommended by CISA, will not prevent attack, but raise physical and operational barriers that attackers have to circumvent—using known effective techniques—to gain access to target systems.
  - As voters, we cannot expect every single jurisdiction to properly and completely implement these countermeasures and to completely guard against attacks where attackers use access gained from insiders (usually inadvertently, e.g., via phishing)
- Disk images of EMS products are already known to be "in the wild," (i.e., previously released on the so-called "dark web") and available as a resource to attackers.
  - Advanced attackers do not need the information gained from these images, in order to construct successful attacks that alter election outcomes.
  - Security researchers have confirmed that the images contain information that can enable a larger set of adversaries to construct additional exploit techniques.[5]
  - However, broader disclosure and distribution of deeper amounts of election technology IP—such as what was experienced in Coffee County—greatly expands the scope of opportunity for development of more attack methods and mechanisms, and we believe this is game-changing for the threat environment.

The Consequences of Disclosures

Given this threat environment, it must be unacceptable to release such vendor IP, including, but not limited to disk images, because they provide a powerful increment of information to broaden the range of exploits on voting systems used in elections. The recent unauthorized disclosure and the apparent quantity and quality of software, data, and other artifacts could trigger a tsunami of new attack methods, means, and mechanisms. In fact, these disclosures (and worse, publication) provide massive updates to materials already "in the wild" and represent a clear and present danger to election infrastructure protection and security.

---

[5] Imaging generally means a binary or executable image that may look intimidating to the untrained eye, but is actually the entry point for significant vulnerability analysis. While not immediately "readable" for understanding operational capabilities, the binary or executable code can be parsed and read by readily available reverse engineering tools (including disassemblers and reverse compilers). In fact, such tools are regularly used in introductory computer science college courses. We also note that many commentators and recreational programmers tend to focus on software source code (which suggests reverse compilation); however, disassemblers are more useful for analysis because they assign English language tags and commands. Those are used to answer the analysts' questions (bear in mind that vulnerability discovery is a series of experiments—the analyst asks whether the system checks some value and then hunts for the code that answers that particular question).

In practice, and to the casual observer, this may appear to be poking around in the darkness of an incomprehensible string of binary code (1s and 0s). However, in fact, once that process is underway and one begins to identify APIs, libraries, and hard-coded information, then standard tests can be applied (again, as in lab work in every computer science curriculum) and the process of discovery and enlightenment accelerates.

However, there is another related concern. An additional, more recent, factor is that some election administration or operations insiders appear to be at least abetting, and at worst, performing abuse of voting systems for some (nefarious and/or partisan) agenda. As a result:

- More access to disk images and disclosed (or worse, published) content means more opportunity to develop new exploits in addition to those that do not require such access.
- More exploits become available, including exploits that can be used by larger numbers of less sophisticated attackers operating locally.
- An increased pool of exploits and attackers, when combined with insider access (i.e., physical infrastructure security is compromised), creates many more opportunities for effective attacks.

Returning to the original questions, it's not necessary to assess the increased risk or likelihood of an actual attack, or to assess the likelihood of a larger pool of attackers or insiders. It is simply the *possibility* of enabling a larger number of attackers with a larger array of exploits, that should be enough to take measures to prevent unauthorized release of disk images, data dumps, or other technical internals of voting system products that have been shown to be rife with security issues.

Conclusions

Further unauthorized release and publication of election technology IP must be prevented because they can, and likely will facilitate and foster future attacks on election trust through either cyber-weapons or disinformation weapons.

Assessing the *likelihood* of such attacks or their impact is not required; the threat environment is so daunting, and public trust in U.S. elections is so fragile, that any amplification of any nature must be prevented. In any event, once these disclosures have occurred, significant efforts and resources must be deployed to immediately mitigate the misinformation likely to be created and amplified to further deteriorate public confidence.

Finally, unauthorized disclosures that lead to such amplifications must not be tolerated, and those responsible held accountable to the full extent of the law. And a related topic that emerges for consideration elsewhere is strengthening laws, regulations, and penalties for such compromises of what amounts to national security assets given election technology is critical infrastructure.

In closing, we also find it important to add the following clarification. None of the content in this statement about the dangers of unauthorized intellectual property releases (e.g., disk images[6] et al) is meant to suggest, support, or make any case for any claim that the 2020 election may have been tampered with, altered, hacked, or rigged. Such is absolutely *not* the case because there is no evidence whatsoever that any such digital subversive act occurred in any system in any of the jurisdictions where such claims were made.

[6] We note in passing that disk imaging is a detailed examination—an intimate act of inspection. The very existence of an image file discloses much about the physical security or lack thereof in the vendor's development environment. The OSET Institute is a strong proponent of high assurance engineering for the design and development of the critical infrastructure of election administration technology. Disk imaging is a good example of why.

Moreover, for Georgia, the durable paper ballot of record remains available and was used to verify the results through recounting. However, that process itself has not been without its own complications.[7]

We also observe that *none* of this statement about the unauthorized disclosure of election technology IP has anything to do with the court-sealed report by University of Michigan's Dr. Halderman subject of pending GA litigation, which addresses separate vulnerabilities in other parts of the Dominion election system.

# # # # #

[7] We do not mean to suggest that, in the case of Georgia, the Ballot Marking Device (BMD) printout is necessarily trustworthy and or that there are routine risk-limiting audits or recounts of all contests everywhere. That's simply not the case. Our point here is that in the face of unsupported claims about subversive manipulation of voting machines in 2020, there was other physical evidence to consider in order to verify the results.

And the over-arching point is that unauthorized acquisition, disclosure, or publication of voting system vendors' intellectual property in the form if disk images or any other means in order to attempt to prove a theory about election hacking is absolutely *not* the way to do so.

Further, to the nuance of Georgia ballot counting and recounting, one of the main issues in the *Curling v. Raffensperger* case as we understand it, is that the BMDs might not print voters' selections accurately, either on the plaintext or the QR code. Moreover, Georgia only audits one contest every 2-years, and candidly we are not convinced their audits are rigorously conducted. Yet, we need not single out Georgia on that count; in fact, most states do not perform post-election results audits in a way that— even if the paper trail were demonstrably trustworthy —has any chance of correcting wrong outcomes, much less a guaranteed minimum chance (*limiting risk*). And to that end, Georgia does not appear to rigorously keep track of the paper (or memory cards, etc.), which is aggravated by the fact that in Georgia the QR codes are the legal official vote for counts and recounts. So, yes, paper ballots are the very best way to start toward a post-election verification of the outcome and an excellent means to thwart "kraken" about subversive activities in the machinery. However, the reliability of the paper cannot be presumed absent certain processes, procedures, and clear evidence of voter intent in the ballot as cast.